CYSEC Cybersecurity TU Darmstadt | System Security Lab | TECHNISCHE UNIVERSITÄT DARMSTADT

# HiWi Stelle – Maschinelles Lernen zur Erkennung von Laufzeitangriffen

## Hintergrund

Die Sicherheit eingebetteter Systeme wird im Zuge von zunehmenden Cyber-Sicherheitsangriffen immer wichtiger. Die Erkennung verschiedener Klassen von Laufzeitangriffen mit minimaler Latenzzeit ist in der heutigen Welt entscheidend für den Aufbau und die Pflege eines sicheren und vertrauenswürdigen Systems.

Der Zweck unserer Arbeit besteht darin, aus der Ausführung eines Prozessors eines gegebenen Anwendungscodes zur Laufzeit abzuleiten, ob die Ausführung gutartig oder kompromittiert ist. Dies erfordert das Sammeln eines repräsentativen Datensatzes von normalen Ausführungsverfolgungen und das Trainieren einer LSTM-Architektur auf diesen. Wir wollen mehrere Exploits erstellen und unsere Architektur gegen sie testen. In unserem System Security Lab wollen wir die Wirksamkeit eines solchen Ansatzes für Low-End-Embedded-Geräte untersuchen und bewerten.

## Anforderungen

- Hintergrund und Interesse am maschinellen und tiefen Lernen, insbesondere LSTMs
- Vertrautheit mit der Programmierung in Python
- Vertrautheit mit TensorFlow und Keras
- Vertrautheit / Bereitschaft, mit RISC-basierten und x86-Prozessorarchitekturen sowie Cross-Compilierungs- und Emulationswerkzeugen zu lernen
- Ein Problemlöser!

## Kontakt

Wenn Du Teil dieses interessanten Projekts werden und an der Forschung auf dem neuesten Stand teilnehmen möchten, sende bitte Deine Bewerbung (Lebenslauf, Zertifikat (e) und etwaige unterstützende Dokumente) per E-Mail an:

Ghada Dessouky
ghada.dessouky@trust.tu-darmstadt.de

## Position

- Sofort verfügbar

AK Professor Dr.-Ing. Ahmad-Reza Sadeghi
Gebäude S4|14 (CASED Gebäude)
Mornewegstraße 30
64293 Darmstadt
https://www.trust.informatik.tu-darmstadt.de

August 2018